Managing AI Projects in the U.S.: Are Emerging Privacy Laws Keeping Pace?

Author: Yixing Jing

About the Author:

Yixing Jing is an independent legal researcher whose work explores the intersection of AI governance, privacy regulation, and technology ethics. He holds an LL.M. from Northeastern University, a Bachelor of Laws from Gansu University of Political Science and Law, and is pursuing Project Management studies at Boston University. He is also a Certified Information Privacy Professional (CIPP/US). His writing evaluates how U.S. privacy law frameworks adapt to the challenges posed by AI development, emphasizing legal accountability and risk-based compliance.

Abstract: This article analyzes the state of privacy laws in the United States and proposes whether they are adequate in the current progress and introduction of artificial intelligence technologies. It discusses how privacy and transparency obligations should be managed concerning the use of AI through methodologies in project management and addressing legal requirements currently in force and those upcoming. From these definitions, this analysis comprehends how AI development processes intertwine with legal concerns, the significance of ethics in technological creations, and prospects of future regulations that can resolve gaps between AI advancement and privacy. Furthermore, the paper emphasizes integrating privacy into a system's life cycle, development, and deployment using PbD and transparency tools like XAI. The article encourages the integration of legal scholars and policymakers alongside the developers of AI technologies to establish a uniform regime of regulations that can embody the best approaches and processes to facilitate the latter's development while preventing the infringement of individuals' privacy rights. The presented material also emphasizes that AI regulation should be based on advanced, flexible, and timely strategies to meet this need.

Introduction: The Regulatory and Ethical Imperatives of AI Privacy

AI technology is being adopted in various fields, such as healthcare, finance, law enforcement, etc. As with most emerging technologies, AI comes with significant risks to privacy and transparency, more of which appear information-based and utilize large datasets that sometimes include personally identifiable information.[1] It is, therefore, imperative to look at how privacy laws are being developed and applied to address these problems about artificial intelligence. Some of the U.S. lacks a unified nationwide legal regime governing AI privacy as multiple institutions establish different rules regulating its use.[2] However, the protection comes from multiple state laws, federal regulations, and rules specific to certain sectors. This paper looks at the extent to which new privacy laws enable innovation in AI and how privacy and transparency requirements can be integrated into an AI project and project management.

I. Legal Frameworks Governing AI Privacy in the USUS.

The U.S. privacy law has been mainly sectoral and without a common federal framework for new technologies like AI. Federal and state-level regulations are constantly evolving in response to the potential of AI to compromise individuals' data privacy.[3]

Federal Regulations

[1] ElBaih, Mohamed. "The role of privacy regulations in ai development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI)." *Available at SSRN 4589207* (2023). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4589207

[2] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014), https://www.columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/ (last accessed Apr. 3, 2025).

[3] Al-Maamari, Amir. "Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, US, UK, and China." *arXiv preprint arXiv:2503.05773* (2025). https://arxiv.org/abs/2503.05773

Federal legal requirements concerning privacy concerning artificial intelligence are sectoral, and some of the laws include the Health Insurance Portability and Accountability Act HIPAA for health information, the Children's Online Privacy Protection Act COPPA for children's data, and the California Consumer Privacy Act CCPA for consumer data. The Federal Trade Commission (FTC) also safeguards privacy in many sectors by its authority over unfair and deceptive practices.[4] However, these laws do not address the issues arising from using AI systems as they tend to function in subtly complex ways that are difficult for users and lawmakers to understand. In furtherance of this example, HIPAA exists to govern the privacy of health care information but does not tackle the issue of how AI systems, which can process large volumes of health-related information, should be regulated for privacy.[5] Likewise, the CCPA fails to consider how data is collected through algorithm use and thus does not comprehensively protect the claims of AI data use. As one recent study shows, such restrictions are inadequate while considering the scale and density of data used by AI-based systems and, therefore, do not consider many AI-driven cases that may not be PII but are still privacy-sensitive.

State-Level Privacy Laws

Another significant advancement of USUS privacy law is the enactment of state laws, especially the CCPA in California and the more recent CPRA. These laws empower the consumer and grant them specific rights over their data, referred to as the data subject rights, which are the rights to access, delete, and opt out of use.[6] The CCPA and the CPRA also require companies to inform

---

[4] Lund, Brady, Zeynep Orhan, Nishith Reddy Mannuru, Ravi Varma Kumar Bevara, Brett Porter, Meka Kasi Vinaih, and Padmapadanand Bhaskara. "Standards, frameworks, and legislation for artificial intelligence (AI) transparency." *AI and Ethics* (2025): 1-17. https://link.springer.com/article/10.1007/s43681-025-00661-4.

[5] Liliana Lizarazo Rodríguez & Benjamin Müller, *Governing AI through Privacy Law: A Comparative Perspective*, 12 Eur. J. Risk Regul. 355 (2021), https://doi.org/10.1017/err.2021.30 (last accessed Apr. 3, 2025).

[6] Gambhir, Ankit, Neha Jain, Medhavi Pandey, and Simran. "Beyond the Code: Bridging Ethical and Practical Gaps in Data Privacy for AI-Enhanced Healthcare Systems." In *Recent Trends in Artificial Intelligence Towards a*

consumers how their personal information is collected, used, and shared. However, these state laws have shortcomings and only apply to a few civil liberties. However, the CCPA only covers businesses that operate in California, does not extend its authority beyond California, and does not address the privacy implications of AI systems in full due to its narrow focus on automated decision-making systems. However, given the decentralized, global nature of developing AI technologies, these state-level frameworks may not adequately protect user data.

The Federal Trade Commission (FTC) and Enforcement

FTC has been responsible for enforcing privacy provisions in the United States since its early days. To date, the agency has concentrated on the following: · Shielding the consumers from deceptive practices in society, including those involving AI systems. The FTC provides specific general guidelines for these firms regarding transparency and accountability, especially concerning AI, but there have been no dedicated policies on this particular technology to date.[7] It raises concerns about how the current legal regime can effectively mitigate privacy risks that arise from AI solutions. The commission is also hamstrung because no comprehensive CoN privacy law could offer a harmonized structure to enforcement across different states and sectors. For example, In the Matter of Everalbum, Inc., the FTC looked into how an AI-powered photo storage company used facial recognition technology and failed to disclose these practices to the users sufficiently.[8]

The Proposed National Privacy Framework

Smart World: Applications in Industries and Sectors, pp. 37-65. Singapore: Springer Nature Singapore, 2024.

[7] Christopher Kuner et al., *Machine Learning & Data Protection: Risk-Based Approaches*, 10 Int'l Data Priv. L. 3 (2020), https://doi.org/10.1093/idpl/ipz024 (last accessed Apr. 3, 2025).

[8] Megan Gray, *Understanding the Role of AI in Privacy Governance*, 42 Berkeley Tech. L.J. 85 (2022), https://btlj.org/data/articles2022/vol37/37_1/Gray_Final_042622.pdf (last accessed Apr. 3, 2025).

Some of the proposed federal privacy laws include the American Data Privacy Protection Act, which provides a national framework for privacy regulation. This law addresses companies' use of intellectual property in implementing artificial intelligence and the human right to privacy. However, the following proposals have not been wholly codified into law to date, meaning there are significant gaps in regulation. If such frameworks are to be passed, these could help AI developers understand where privacy and transparency obligations lie and address these throughout AI processes.

II. Managing Privacy and Transparency Obligations in an AI Project

AI development is frequently iterative, aligned with agile project management or similar approaches that encourage fast-paced work.[9] However, privacy and transparency concerns are usually not considered within these frameworks, and this can pose a challenge in compliance or may result in the consumers suffering the consequences. Privacy integration into AI projects means a paradigm shift in how AI developers develop data handling and algorithms.[10] This shift requires implementing preventive measures that will integrate privacy and transparency as foundational elements marking the AI development life cycle and not as secondary notions considered after the base development is established.

Privacy by Design

[9] Humerick, Matthew. "Taking AI personally: how the EU must learn to balance the interests of personal data privacy & artificial intelligence." *Santa Clara High Tech. LJ* 34 (2017): 393. https://heinonline.org/HOL/LandingPage?handle=hein.journals/sccj34&div=19&id=&page=.

[10] Atata, Bashirat Bukola. "The AI Privacy Paradox: A Comparative Analysis of EU And U.S Approaches to Regulating Artificial Intelligence and Protecting Personal Data." https://www.researchgate.net/profile/Bashirat-Atata/publication/384243920_THE_AI_PRIVACY_PARADOX_A_COMPARATIVE_ANALYSIS_OF_EU_AND_US_APPROACHES_TO_REGULATING_ARTIFICIAL_INTELLIGENCE_AND_PROTECTING_PERSONAL_DATA/links/66f0a5a1c0570c21feb6a2ed/The-Ai-Privacy-Paradox-A-Comparative-Analysis-Of-Eu-And-Us-Approaches-To-Regulating-Artificial-Intelligence-And-Protecting-Personal-Data.pdf

Privacy by Design (PbD) is considered a cornerstone principle in the current framework of privacy law and introduces the notion that privacy should be a consideration when conceptualizing technology.[11] This involves privacy in every AI chain, including data acquisition, model building, and application of the actual system. For example, AI systems can apply data anonymization and data encryption techniques to avoid leakage or exposure of user data that may violate users' privacy.[12] PbD also includes principles of least privilege, where an AI system is given access only to the data required to perform the intended tasks to reduce privacy risks as much as possible. Moreover, PbD involves the minimization of data collection, including the collection of data essential for the system's functioning only.[13] This minimizes the chances of data being breached since there is less data, which could be exploited if there was a security breach.

Transparency and Explainability in AI

One big problem in AI is the explicability of the results and decision-making, especially as many AI tools and techniques, like deep learning algorithms, are opaque at their core.[14] This lack of

---

[11] Shackelford, Scott J., and Rachel Dockery. "Governing AI." *Cornell JL & Pub. Pol'y* 30 (2020): 279. https://heinonline.org/HOL/LandingPage?handle=hein.journals/cjlpp30&div=14&id=&page=

[12] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014), https://www.columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/ (last accessed Apr. 3, 2025).

[13] Kanabar, Vijay. *The AI Revolution in Project Management: Elevating Productivity with Generative AI*. Sams Publishing, 2023. https://books.google.co.ke/books?hl=en&lr=&id=sXriEAAAQBAJ&oi=fnd&pg=PT14&dq=Managing+AI+Projects+in+the+U.S.:+Are+Emerging+Privacy+Laws+Keeping+Pace%3F&ots=mPg1O-K8_y&sig=mq7GFZBQImcmenQFnTTPS8-3lKg&redir_esc=y#v=onepage&q&f=false.

[14] Mbah, Geraldine O. "Data privacy in the era of AI: Navigating regulatory landscapes for global businesses." (2024). https://www.researchgate.net/profile/Geraldine-Mbah/publication/387025413_Data_privacy_in_the_era_of_

transparency can pose a problem for consumers and regulators to comprehend how personal data is processed or how decisions are arrived at. To address the problem of AI fairness, the concept of Explainable AI (XAI) is designed to make AI-generated choices more understandable.[15] This way, AI developers can ensure that the end-user has an insight into how the decision was made by the AI, especially in sensitive areas such as healthcare, law enforcement, and finance in re Facebook Biometric Info. Also, using transparency in such AI systems ensures that individuals can question any decision-making outcomes or results considered unfair or wrong.[16] This is because most countries' data protection laws also exist in light of the General Data Protection Regulation, which states that data subjects must understand how decisions are made about them.

Risk Management and Legal Compliance

For the AI system to comply with privacy laws, the AI project managers should consider incorporating risk management practices into their project management frameworks. This includes carrying out DPIAs to assess the data processing activity's risk and ensure that privacy risks are adequately managed.[17] DPIAs are helpful in AI as they can aid in discovering how AI

AI_Navigating_regulatory_landscapes_for_global_businesses/links/675c9d8cebc8f979702cae20/Data-privacy-in-the-era-of-AI-Navigating-regulatory-landscapes-for-global-businesses.pdf

[15] Gambhir, Ankit, Neha Jain, Medhavi Pandey, and Simran. "Beyond the Code: Bridging Ethical and Practical Gaps in Data Privacy for AI-Enhanced Healthcare Systems." In *Recent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors*, pp. 37-65. Singapore: Springer Nature Singapore, 2024.

[16] Kanabar, Vijay. *The AI Revolution in Project Management: Elevating Productivity with Generative AI*. Sams Publishing, 2023. https://books.google.co.ke/books?hl=en&lr=&id=sXriEAAAQBAJ&oi=fnd&pg=PT14&dq=Managing+AI+Projects+in+the+U.S.:+Are+Emerging+Privacy+Laws+Keeping+Pace%3F&ots=mPg1O-K8_y&sig=mq7GFZBQImcmenQFnTTPS8-3lKg&redir_esc=y#v=onepage&q&f=false.

[17] Gilani, Syed Raza Shah, Ali Mohammed Al-Matrooshi, and Muhammad Haroon Khan. "Right of privacy and the growing scope of artificial intelligence." *Current Trends in Law and Society* 3, no. 1 (2023): 1-11. https://journals.internationalrasd.org/index.php/ctls/article/view/1633

algorithms affect the privacy of individuals and human rights. DPIAs also allow AI developers to evaluate the efficiency of data protection measures regularly and modify the applied systems according to the appearance of new threats. There can also be measures to automatically or periodically review the AI systems for compliance with privacy laws. These audits should address both the technology used and the utilization of the system, such as data processing, how operations are explained, and how customers provide consent regarding the AI usage, to verify that developers respect data privacy and protection standards.

III. Challenges and Gaps in USUS Privacy Law and AI Development

The evaluation of AI in diverse industries is promising, yet the current state of privacy laws in the United States has the following barriers to regulating artificial intelligence technologies.[18] These challenges include fluctuating legal systems that do not comply with the existing laws, inadequate coverage of the rules and policies, and AI's ever-evolving field and technology.

Inconsistencies between State and Federal Law

One impediment to the development of AI is the highly fragmented nature of the privacy laws in the United States. That is why each state can adopt its laws concerning privacy, which results in the absence of a unified network of laws. Such a situation presents compliance challenges to organizations doing business across different states and undermines the progress toward developing a uniform standard for artificial intelligence.[19] Writing for the chorus, they argued

[18] Humerick, Matthew. "Taking AI personally: how the EU must learn to balance the interests of personal data privacy & artificial intelligence." *Santa Clara High Tech. LJ* 34 (2017): 393. https://heinonline.org/HOL/LandingPage?handle=hein.journals/sccj34&div=19&id=&page=.

[19] Calo, Ryan. "Artificial intelligence policy: a primer and roadmap." *UCDL Rev.* 51 (2017): 399. https://heinonline.org/HOL/LandingPage?handle=hein.journals/davlr51&div=18&id=&page=

that when there is no unified federal privacy law, AI developers may have to deal with many different laws, thus making it challenging to ensure compliance with privacy and transparency requirements.

AI-Specific Privacy Concerns

Some AI applications, such as facial recognition and predictive algorithms, pose privacy risks not covered by current legal acts. For example, facial recognition technology — incorporated into security and surveillance systems — causes concerns about mass surveillance and biometric data collection.[20] For instance, the algorithms applied in criminal justice digital bodies can reinforce prejudice and discrimination against minorities. These applications entail particular legal structures to regulate privacy that differ from Artificial Intelligence and not the current laws that have not been developed to cater to these technologies.

The Role of Ethics in Legal Regulation

Moreover, artificial intelligence is a matter of legal regulation and ethical considerations. Specifically, as AI systems become more pervasive, developers need to ensure that AI algorithms are equitable and non-biased, not biased. This means that legal frameworks can force transparency on how data is processed, and automated decisions are made, thus supporting ethical principles.[21] However, there is a growing awareness that applying the law cannot solve a broader range of problems associated with using AI, including questions of fairness and

[20] Al-Maamari, Amir. "Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, US, UK, and China." *arXiv preprint arXiv:2503.05773* (2025). https://arxiv.org/abs/2503.05773

[21] Christopher Kuner et al., *Machine Learning & Data Protection: Risk-Based Approaches*, 10 Int'l Data Priv. L. 3 (2020), https://doi.org/10.1093/idpl/ipz024 (last accessed Apr. 3, 2025).

corporate responsibility. From the general perspective, Timnit Gebru advances a compelling argument on AI Ethics and Accountability in the Age of Automation in AI.[22]

IV. Recommendations for Improving AI Privacy Regulation

Some changes are required to bring privacy law in congruence with the advanced world of artificial intelligence.[23] These should meet AI technologies' new challenges and guarantee that privacy considerations become part of AI engineering.

Harmonizing State and Federal Laws

This raises the question of whether there is a real need for federal privacy legislation that would provide a base for states. This exemption would benefit businesses operating across several stations because it would outline general rules that apply to all of them instead of having to navigate the laws of each state, which may be confusing or contradictory.[24] This should cover algorithmic accountability, biometrics and other sensitive data, and artificial intelligence decision-making. Unknown to many, legal frameworks related to POT are still a work in progress, and the present legal structure constitutes a patchwork of laws spread across various states. The federal framework would help avoid duplication and confusion and suggest how to

---

[22] Paul M. Schwartz, *Privacy by Design: A Counterfactual Analysis of U.S. and EU Approaches*, 17 Wash. J.L. Tech. & Arts 283 (2021), https://digitalcommons.law.uw.edu/wjlta/vol17/iss3/3/ (last accessed Apr. 3, 2025).

[23] Mihyawi, Sameer. *The Artificial Intelligence Era Between Governance and Our Privacy Protection*. Sameer Mihyawi, 2024. https://books.google.co.ke/books?hl=en&lr=&id=Bs85EQAAQBAJ&oi=fnd&pg=PR1&dq=Managing+AI+Projects+in+the+U.S.:+Are+Emerging+Privacy+Laws+Keeping+Pace%3F&ots=WMCW5jai6W&sig=ETLBpVIHrMaaAPSVFF0akAKYKKs&redir_esc=y#v=onepage&q&f=false.

[24] Gilani, Syed Raza Shah, Ali Mohammed Al-Matrooshi, and Muhammad Haroon Khan. "Right of privacy and the growing scope of artificial intelligence." *Current Trends in Law and Society* 3, no. 1 (2023): 1-11. https://journals.internationalrasd.org/index.php/ctls/article/view/1633

proceed with enforcement. It must also be capable of adapting to the evolving developments in artificial intelligence while at the same time preserving the rights of individuals to privacy.

Incentivizing Privacy-First Design

The government can encourage privacy-enhancing designs by allocating tax credits or other forms of compensation to AI businesses that implement adequate privacy measures. These incentives ensure that privacy integration is a primary approach when developing artificial intelligence systems and does not become an add-on feature.[25] It was also observed that such initiatives might help foster a privacy consciousness among the developers, who tend to see privacy not as anathema to development but as a strategic edge that could be leveraged. Promoting privacy-first models will preserve users' freedom and build trust in AI technologies among people.[26]

Increasing International Cooperation

AI is a global issue, and that means the regulations concerning the protection of privacy must be made universally and within a coordinated manner.[27] The United States can cooperate with the

---

[25] Calo, Ryan. "Artificial intelligence policy: a primer and roadmap." *UCDL Rev.* 51 (2017): 399. https://heinonline.org/HOL/LandingPage?handle=hein.journals/davlr51&div=18&id=&page=

[26] Payton, Theresa, and Ted Claypoole. *Privacy in the age of Big data: Recognizing threats, defending your rights, and protecting your family*. Rowman & Littlefield, 2023. https://books.google.co.ke/books?hl=en&lr=&id=1nGgEAAAQBAJ&oi=fnd&pg=PR5&dq=Managing+AI+Projects+in+the+U.S.:+Are+Emerging+Privacy+Laws+Keeping+Pace%3F&ots=2fej1-AJkV&sig=uw0ZuyHRrGZWjh9D8y8FWH9y6dI&redir_esc=y#v=onepage&q&f=false

[27] Atata, Bashirat Bukola. "The AI Privacy Paradox: A Comparative Analysis of EU And U.S Approaches to Regulating Artificial Intelligence and Protecting Personal Data." https://www.researchgate.net/profile/Bashirat-Atata/publication/384243920_THE_AI_PRIVACY_PARADOX_A_COMPARATIVE_ANALYSIS_OF_EU_AND_US_APPROACHES_TO_REGULATING_ARTIFICIAL_INTELLIGENCE_AND_PROTECTING_PERSONAL_DATA/links/66f0a5a1c0570c21feb6a2ed/The-

EU and other global organizations to establish international standards for AI that will enforce privacy rights regardless of geographical location. Since the approaches can be harmonized in these areas, countries can work together to combat privacy issues in a way that does not bring about disparity or confusion of privacy laws across borders.

Promoting Consumer Education and Engagement

Last but not least, increasing awareness about consumer rights and making them more active in matters concerning AI privacy will go a long way in enhancing the privacy of individuals.[28] The government should help individuals understand how their info is processed by AI and their rights today and under future laws and regulations. One possible solution is to ensure that the significance of AI is well-informed by the public, with high expectations from developers and regulators.[29] Education, communication, and providing means for exercising these rights comprehensibly and concisely will go a long way to engage consumers and improve privacy.

V. Conclusion: The Path Forward for AI and Privacy Law in the USUS.

Current regulation of AI privacy is a work in progress in the United States, but some critical loopholes persist. New state and federal statutes offer some protection to individuals who have had their privacy breached. Still, they remain inadequate in solving the latest issues arising from

---

Ai-Privacy-Paradox-A-Comparative-Analysis-Of-Eu-And-Us-Approaches-To-Regulating-Artificial-Intelligence-And-Protecting-Personal-Data.pdf

[28] ElBaih, Mohamed. "The role of privacy regulations in ai development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI)." *Available at SSRN 4589207* (2023). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4589207

[29] Al-Maamari, Amir. "Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, US, UK, and China." *arXiv preprint arXiv:2503.05773* (2025). https://arxiv.org/abs/2503.05773

using artificial intelligence.[30] Applying protective measures to individuals' data is crucial to developing AI project management and establishing relevant rules, providing the USUS with a robust ethical structure to implement AI solutions safely. In the future, we will have to see both policymakers and the developers of the technologies come together to ensure that there is a growing set of rules that can govern the use of Artificial intelligence and relate to the expanding market while protecting consumers in this ever-evolving world.[31]

[30] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014), https://www.columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/ (last accessed Apr. 3, 2025).

[31] Porter, David J., Michelle K. Lee, Andrei Iancu, Carl Domino, James C. Cooper, James Boyajian, Shawn D. Hamacher, Ognian Shentov, and Michelle Roberts. "Artificial Intelligence and Big Data Innovations: Navigating the Technology World of the near Future." *U. Dayton L. Rev.* 45 (2020): 1. https://heinonline.org/HOL/LandingPage?handle=hein.journals/udlr45&div=4&id=&page=

Bibliography

Al-Maamari, Amir. "Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, US, UK, and China." *arXiv preprint arXiv:2503.05773* (2025). https://arxiv.org/abs/2503.05773

Atata, Bashirat Bukola. "The AI Privacy Paradox: A Comparative Analysis of EU And U.S Approaches to Regulating Artificial Intelligence and Protecting Personal Data." https://www.researchgate.net/profile/Bashirat-Atata/publication/384243920_THE_AI_PRIVACY_PARADOX_A_COMPARATIVE_ANALYSIS_OF_EU_AND_US_APPROACHES_TO_REGULATING_ARTIFICIAL_INTELLIGENCE_AND_PROTECTING_PERSONAL_DATA/links/66f0a5a1c0570c21feb6a2ed/The-Ai-Privacy-Paradox-A-Comparative-Analysis-Of-Eu-And-Us-Approaches-To-Regulating-Artificial-Intelligence-And-Protecting-Personal-Data.pdf

Calo, Ryan. "Artificial intelligence policy: a primer and roadmap." *UCDL Rev.* 51 (2017): 399. https://heinonline.org/HOL/LandingPage?handle=hein.journals/davlr51&div=18&id=&page=

Christopher Kuner et al., *Machine Learning & Data Protection: Risk-Based Approaches*, 10 Int'l Data Priv. L. 3 (2020), https://doi.org/10.1093/idpl/ipz024 (last accessed Apr. 3, 2025).

Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014), https://www.columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/ (last accessed Apr. 3, 2025).

ElBaih, Mohamed. "The role of privacy regulations in ai development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI)." *Available at SSRN 4589207* (2023). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4589207

Gambhir, Ankit, Neha Jain, Medhavi Pandey, and Simran. "Beyond the Code: Bridging Ethical and Practical Gaps in Data Privacy for AI-Enhanced Healthcare Systems." In *Recent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors*, pp. 37-65. Singapore: Springer Nature Singapore, 2024.

Gilani, Syed Raza Shah, Ali Mohammed Al-Matrooshi, and Muhammad Haroon Khan. "Right of privacy and the growing scope of artificial intelligence." *Current Trends in Law and Society* 3, no. 1 (2023): 1-11. https://journals.internationalrasd.org/index.php/ctls/article/view/1633

Humerick, Matthew. "Taking AI personally: how the EU must learn to balance the interests of personal data privacy & artificial intelligence." *Santa Clara High Tech. LJ* 34 (2017): 393. https://heinonline.org/HOL/LandingPage?handle=hein.journals/sccj34&div=19&id=&page=.

Kanabar, Vijay. *The AI Revolution in Project Management: Elevating Productivity with Generative AI*. Sams Publishing, 2023. https://books.google.co.ke/books?hl=en&lr=&id=sXriEAAAQBAJ&oi=fnd&pg=PT14&dq=Managing+AI+Projects+in+the+U.S.:+Are+Emerging+Privacy+Laws+Keeping+Pace%3F&ots=mPg1O-K8_y&sig=mq7GFZBQImcmenQFnTTPS8-3lKg&redir_esc=y#v=onepage&q&f=false.

Liliana Lizarazo Rodríguez & Benjamin Müller, *Governing AI through Privacy Law: A Comparative Perspective*, 12 Eur. J. Risk Regul. 355 (2021), https://doi.org/10.1017/err.2021.30 (last accessed Apr. 3, 2025).

Lund, Brady, Zeynep Orhan, Nishith Reddy Mannuru, Ravi Varma Kumar Bevara, Brett Porter, Meka Kasi Vinaih, and Padmapadanand Bhaskara. "Standards, frameworks, and legislation for artificial intelligence (AI) transparency." *AI and Ethics* (2025): 1-17. https://link.springer.com/article/10.1007/s43681-025-00661-4.

Megan Gray, *Understanding the Role of AI in Privacy Governance*, 42 Berkeley Tech. L.J. 85 (2022), https://btlj.org/data/articles2022/vol37/37_1/Gray_Final_042622.pdf (last accessed Apr. 3, 2025).

Mbah, Geraldine O. "Data privacy in the era of AI: Navigating regulatory landscapes for global businesses." (2024). https://www.researchgate.net/profile/Geraldine-Mbah/publication/387025413_Data_privacy_in_the_era_of_AI_Navigating_regulatory_landscapes_for_global_businesses/links/675c9d8cebc8f979702cae20/Data-privacy-in-the-era-of-AI-Navigating-regulatory-landscapes-for-global-businesses.pdf

Mihyawi, Sameer. *The Artificial Intelligence Era Between Governance and Our Privacy Protection*. Sameer Mihyawi, 2024. https://books.google.co.ke/books?hl=en&lr=&id=Bs85EQAAQBAJ&oi=fnd&pg=PR1&dq=Managing+AI+Projects+in+the+U.S.:+Are+Emerging+Privacy+Laws+Keeping+Pace%3F&ots=WMCW5jai6W&sig=ETLBpVIHrMaaAPSVFF0akAKYKKs&redir_esc=y#v=onepage&q&f=false.

Payton, Theresa, and Ted Claypoole. *Privacy in the age of Big data: Recognizing threats, defending your rights, and protecting your family*. Rowman & Littlefield, 2023. https://books.google.co.ke/books?hl=en&lr=&id=1nGgEAAAQBAJ&oi=fnd&pg=PR5&dq=Managing+AI+Projects+in+the+U.S.:+Are+Emerging+Privacy+Laws+Keeping+Pace%3F&ots=2fej1-AJkV&sig=uw0ZuyHRrGZWjh9D8y8FWH9y6dI&redir_esc=y#v=onepage&q&f=false

Porter, David J., Michelle K. Lee, Andrei Iancu, Carl Domino, James C. Cooper, James Boyajian, Shawn D. Hamacher, Ognian Shentov, and Michelle Roberts. "Artificial Intelligence and Big Data Innovations: Navigating the Technology World of the near Future." *U. Dayton L. Rev.* 45 (2020): 1. https://heinonline.org/HOL/LandingPage?handle=hein.journals/udlr45&div=4&id=&page=

Paul M. Schwartz, *Privacy by Design: A Counterfactual Analysis of U.S. and EU Approaches*, 17 Wash. J.L. Tech. & Arts 283 (2021), https://digitalcommons.law.uw.edu/wjlta/vol17/iss3/3/ (last accessed Apr. 3, 2025).

Shackelford, Scott J., and Rachel Dockery. "Governing AI." *Cornell JL & Pub. Pol'y* 30 (2020): 279. https://heinonline.org/HOL/LandingPage?handle=hein.journals/cjlpp30&div=14&id=&page=